



Office of the City Auditor

Business Resumption Report No. 0162

December 20, 2001

The City needs to develop a business resumption plan to ensure that there is a coordinated response to a disaster or unforeseen event that would disrupt critical business functions. While there is a Disaster Recovery Plan that addresses the City's computer network and the equipment within the data center, this Plan is not sufficient to ensure that the City would be able to recover and restore critical computer operations within an appropriate timeframe.

CITY COUNCIL

Mayor
Mary Manross

Council
Cynthia Lukas
Ned O'Hearn
David Ortega
Robert Pettycrew
Tom Silverman
George Zraket



December 20, 2001

"Most Livable City"

U.S. Conference of Mayors

OFFICE OF
CITY AUDITOR

7440 E. FIRST AVENUE
SCOTTSDALE, AZ 85251

(480) 312-7756 PHONE
(480) 312-2634 FAX

To the Most Honorable Mary Manross, Mayor
and Members of the Scottsdale City Council

Transmitted herewith is a report on our evaluation of the City's preparation and readiness to respond to a disaster or unforeseen event that would cause disruption to critical business functions (Report No. 0162).

When completing this work, several issues came to our attention:

- 1) We found that the City's Emergency Response Plan has not been updated since spring 1999. As a result, it does not reflect changes in staffing or equipment that have occurred since the last revision.

The requirement for an emergency services plan is outlined in Scottsdale Revised Code (SRC), Chapter 10. According to SRC Section 10-5, the purpose of this plan is to build preparedness and readiness to ensure coordinated operations in the event of a disaster or other emergency. The plan is considered supplemental to City Code and has the effect of law during a situation in which an emergency is declared. As such, it is imperative that it be kept current, particularly when there are changes within the organization.

- 2) Citywide awareness and training programs are not provided annually and the Emergency Services Director assumes no responsibility for ensuring that departmental plans are current or sufficient.

For a plan to be effective, periodic awareness and training activities need to be undertaken. At a minimum, a citywide training exercise should be provided annually. As well, there needs to be a coordinated effort to ensure that departmental plans, supplemental to the citywide plan, are current and sufficient.

We recommend that the City Council direct the City Manager to instruct the Emergency Services Director to prepare a revised Emergency Response Plan for Council adoption as soon as reasonably feasible. As well, the Emergency Services Director should be instructed to submit a program that will ensure that the Plan is reviewed no less than annually. The program should also include a requirement for an awareness and training activity at least annually. Additionally, the duties of the Emergency Services Director should be expanded to include a requirement to coordinate, and review for sufficiency and consistency, departmental plans that supplement the citywide plan.

- 3) We noted that the City is not maintaining current job descriptions. Job descriptions for positions we reviewed during this audit (IS Support Manager, Emergency Services Officer, Risk Management Director, and Risk Management Manager) have not been updated since 1996. We also noted that the position of IS Support Manager is no longer reflected on the City list of active titles and pay ranges.

We recommend that the City Council instruct the City Manager to direct the Human Resource Systems General Manager to initiate a process to update all job descriptions and ensure that job titles/duties assigned to City employees are correctly reflected in both job descriptions and classifications.

If you need additional information or have any questions, please contact me at 480-312-7756.

Respectfully submitted,



Cheryl Barcala, CPA, CIA, CFE, CGFM, CISA, CISSP
City Auditor

Table of Contents

EXECUTIVE SUMMARY	1
Results In Brief.....	1
Action Plan	3
INTRODUCTION	8
City Needs to Ensure That Critical Business Operations Can Continue to Be Provided.....	12
Information Systems Disaster Recovery Plan Could Be Enhanced	14
The Information Systems Department has Created the Foundation for a Business Resumption Plan	14
Additional Policies and Procedures Would Enhance the Efforts	15
OBJECTIVES, SCOPE, AND METHODOLOGY	18
APPENDIX A	29
Management Response	29

EXECUTIVE SUMMARY

This audit was initiated by the City Auditor's Office as provided under Scottsdale Revised Code §2-120. Preson (Sonny) W. Phillips, Jr. conducted the audit with work beginning in June and concluding in July 2001. The work was conducted in accordance with generally accepted government auditing standards as they relate to expanded scope auditing as required by Article III, Scottsdale Revised Code §2-117 *et seq.*

The objective of the audit was to determine if the City was adequately prepared to respond to a disaster or unforeseen event that caused disruption to the delivery of one or more critical business functions. To reach our conclusion regarding the objective, we used criteria developed by the Information Systems Audit and Control Foundation (ISACF or Foundation) and standards promulgated by DRI International (formally the Disaster Recovery Institute). DRI International is the internationally recognized organization for certification of business continuity professionals (formerly disaster recovery planners). These criteria are considered "best practices" for continuity planning.

Continuity Planning: Process of developing advance arrangements and procedures that enable an organization to respond to an event in such a manner that critical business functions continue without interruption.

Resumption Planning: Process of developing advance arrangements and procedures that enable an organization to respond to an event that last for an unacceptable period of time and return to performing its critical business functions after an interruption.

In this report, the terms "resumption" and "continuity" can be used interchangeably.

Results In Brief

We found that the City has the start of a business resumption plan in the Disaster Recovery Plan maintained by the City's Information Systems Department (IS). This Plan would help facilitate the recovery of the City's computer network, if necessary. However, the Plan, as it currently exists, is not sufficient to ensure timely restoration of computer operations and would not ensure a coordinated response to the disaster or other event.

While the IS Department has undertaken efforts to expand the Plan to include other business functions, there is no organizational directive to departments or divisions to create and maintain business resumption plans for critical

operations. The individual, within the IS Department, responsible for the IS Plan is not charged with the responsibility for developing a citywide business resumption plan, so there is no assurance that disparate efforts within the various City departments are coordinated.

Most importantly, however, we found two situations that place the City at greater risk when dealing with unforeseen events. First, the City does not have a backup site for its computer operations. Currently, the majority of the City's computer network (including the City's voice and data communications infrastructure) is in a computer operations center housed within the Scottsdale Center for the Arts (SCA). It is estimated that it would take a minimum of 30 days to restore portions of this network infrastructure.

Secondly, the City historically purchases information systems equipment through vendors using state contracts or internal contracts that do not include provisions for replacement equipment. These contractual arrangements limit the City's ability to obtain unique pieces of equipment if it became necessary to replace an item on short notice. As such, even if the City were to be able to find alternative space for the equipment, there would be no certainty that the equipment could be located, repurchased, or duplicated in a timely manner.

The Action Plan that follows this summary details our recommendations. Comments from management and their proposed implementation plan are included. The full copy of management's response is located in the Appendix.

Action Plan

No.	Recommendations	Management Response	Status
We recommend that the City Manager develop a business resumption planning program that, at a minimum, includes:			
1	A policy statement that clearly expresses the organization's commitment to ensuring continued business operations. This policy statement should be approved by Council and incorporated into the City Code.	City management is committed to developing, implementing and maintaining a comprehensive management program, which includes planning for continuation of business operations. <i>(Issue #16 in Management Response.)</i>	Implemented at executive level.
2	<p>A requirement for development of a plan that defines the responsibilities, roles, and approval process for the plan. This plan should be based on a risk assessment and impact analysis. At a minimum the plan should include:</p> <ul style="list-style-type: none"> ▪ Guidelines on how to use the plan. ▪ Emergency procedures to ensure safety of all staff members. ▪ Response procedures meant to bring systems back to the condition before the incident or disaster. ▪ Recovery procedures to bring the systems back to the condition before the incident or disaster. ▪ Procedures to secure and reconstruct the site. ▪ Coordination procedures with public authorities. ▪ Communications procedures. ▪ Critical information on continuity teams, affected staff, customers, suppliers, public authorities, and media. 	Management agrees that there is a need for development and regular update of a comprehensive emergency management program, which includes how to continue and resume business during and after an unforeseen event. <i>(Issue #1 in Management Response.)</i>	Plan in development stage.

No.	Recommendations	Management Response	Status
3	Assignment of one individual within the organization with the responsibility of ensuring the development and maintenance of the plan as well as the authority to implement the plan, if necessary. This individual should be required to be a certified business continuity professional.	Executive Assistant Chief Dee Taylor has been delegated lead responsibility for citywide emergency management efforts. Business resumption is a core component of a three-pronged strategy (planning, response, recovery). IS disaster recovery planning efforts are being incorporated into citywide efforts under the operational direction of Mr. Rich Peterson, technology operations manager. <i>(Issue #6 in Management Response.)</i>	Implemented.
4	A requirement that each business unit establish responsibility for plan development, activation, and maintenance.	The new emergency management plan will include individual departmental plans. <i>(Issue #12 in Management Response.)</i>	In planning stages.
5	A requirement for the City's Risk Management Director to participate in the development of the citywide plan.	The Risk Management Director is actively involved in all current emergency management program related activities. He is a member of the Emergency Safety and Preparedness Committee and has provided the assistant city manager with considerable advice and research material upon request. <i>(Issue #15 in Management Response.)</i>	Implemented.

No.	Recommendations	Management Response	Status
We recommend that the City Manager require the IS General Manager/CIO to develop a citywide Information Systems Disaster Recovery Program that would, at a minimum, include:			
1	Identification of a specific individual assigned as the Disaster Recovery Officer, and development of a job description that would include disaster recovery responsibilities. This individual should be required to implement policies and procedures that incorporate all appropriate elements outlined by ISACF. As well, the individual should be required to be a certified business continuity professional.	IS disaster recovery planning efforts are being incorporated into citywide efforts under the operational direction of Rich Peterson, technology operations manager. <i>(Issue #6 in Management Response.)</i>	Implemented.
2	Completion of an enterprise-wide risk assessment of all applications using the City's network or supported by IS to determine minimum acceptable time for recovery of the City's network and/or server farm.	The IS Department's disaster recovery officer is responsible for facilitation of a process which will determine organizational priorities for bringing critical systems back online within a preferred timeframe. <i>(Issue #10 in Management Response.)</i>	Task has been assigned.
3	Development of a best case scenario regarding the time to provide service should the SCA building become inaccessible or sustain sufficient damage to impact portions of the network.	The IS Department disaster recovery consultant will assist with evaluating ways to reduce potential downtime. The IS effort should be completed within 120 days, and a timeline for looking at citywide services is being developed by the ESAP team. <i>(Issue #11 in Management Response.)</i>	IS effort estimated to be completed within 120 days.

No.	Recommendations	Management Response	Status
4	Identification of an alternative computer operations center and development of strategic plans for bringing that site online, if necessary.	IS management is in full support of an alternative site, be it "hot, warm or cold." Initial efforts are underway to identify a "cold site" location. Potential private and/or regional solutions will be evaluated by the IS team and the ESAP committee. <i>(Issue #7 in Management Response.)</i>	Site analysis underway.
5	Renegotiation of current contracts to ensure replacement of critical equipment within an established timeframe.	IS management will partner with the legal and purchasing teams in researching options available through current equipment and third party vendors. Replacement language may be included in any contracts being negotiated in the future if feasible. <i>(Issue #8 in Management Response.)</i>	Under analysis.
6	Development of boilerplate language for inclusion in future contracts for critical technology-related components to ensure availability of replacement equipment.	IS management advises that the City already has a high expectation for timely replacement of hardware though <i>[sic]</i> use of existing maintenance contracts. The department will explore this recommendation in cooperation with the legal and purchasing teams, and anticipates the need for a thorough cost/benefit analysis. The IS department further advises that catastrophic events on a nationwide scale are likely to quickly deplete hardware inventories and the capacity of vendors and knowledge workers, regardless of	Cost-benefit analysis to be undertaken.

No.	Recommendations	Management Response	Status
7	A formal meeting, after each incident or successful resumption, to review recovery procedures and modify the plan, if necessary.	contract language. <i>(Issue #9 in Management Response.)</i> All involved city operations shall be included in debriefings held after each incident. <i>(Issue #13 in Management Response.)</i>	Debriefings will be held after each event.
8	Development and implementation of an annual refresher/awareness program to ensure that employees are aware of specific requirements.	Management agrees that this should be a component of the citywide emergency management program. Additionally, staff has found that "mock drills," based on different scenarios, provide the best opportunity for team members to practice implementing the elements of a disaster recovery plan. These exercises will be continued, at least annually and the Emergency Safety and Preparedness Committee will determine how to improve citywide Emergency Preparedness Training. <i>(Issue #14 in Management Response.)</i>	Effective training is being evaluated and developed by citywide team.

INTRODUCTION

Business resumption planning, the subject of this report, is similar in nature to emergency planning. The City's Emergency Response Plan considers potential disasters that would pose a threat to the safety and well being of City employees, citizens, and property. Chapter 10 of the Scottsdale Revised Code addresses the City's need for a plan to ensure a coordinated response to a community-wide disaster or other emergency.

A business resumption plan is more directly related to the functioning of City operations. It addresses health and safety of City employees but focuses on the recovery and continuation of critical City business operations. Basically, the City's efforts in business resumption planning should provide the City with the ability to respond to an interruption in services, restore critical business functions, and resume providing services within an identified timeframe.

The concept of business resumption planning, in the context of disaster recovery, has been around for almost 30 years. As computers and technology advancements became more integrated into business operations, organizations became concerned about the ability to continue operating if some unforeseen event shut down the computer operations center. Plans focused on recovery of the data center through identification of backup facilities, equipment, and resources. Terms such as "hot site" and "business impact analysis" became part of the planning process.

Hot Site: *An alternate facility that has the equipment and resources to recover the business function (data processing, communications, or other critical business functions) affected by the occurrence of a disaster.*

Warm Site: *An alternate facility that is only partially equipped. A warm site would necessitate acquisition of some components should a disaster occur.*

Cold Site: *An alternate facility without any equipment. Generally, a cold site may be a building with air conditioning and flooring sufficient to house computers, but all other equipment and resources would need to be obtained to make the facility operational.*

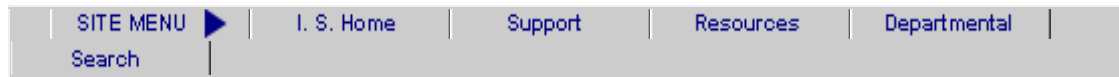
Business Impact Analysis: *A process of analyzing business functions, identifying potential threats, and examining the impact of those threats.*

Disaster Recovery: *The ability to respond to an interruption in services by implementing a disaster recovery plan to restore an organization's critical business functions.*

Similar to other organizations, the City has integrated more computers and technology related infrastructure into the day-to-day operations, but continuity planning is a relatively new concept. It was not until December 1998, when in response to a recommendation made by the City's external auditor (Deloitte and Touche, at that time), that the City completed its first documented computer operations disaster recovery plan for the distributed network. Planning for alternate business continuity strategies received more attention during 1999 as the City prepared for potential impacts of the century date change (the Year 2000 threat or Y2K) with manual contingency plans drafted for critical City functions.

Today, the City's computer infrastructure is still the focus of the City's Disaster Recovery Plan. The City's Chief Information Officer (CIO) has charged an individual in that department with the responsibilities of being the disaster recovery coordinator. This individual ensures that the plan is kept current and has developed the list of assumptions for disaster recovery planning. This list, posted on the City's Intranet, is shown on the following page.

As part of the most recent update, the IS Department engaged the services of the same outside consultant that helped draft the initial plan to assist in expanding the planning to other critical operations. The process was not complete at the time of our review.



The following is a list of assumptions that will have an impact on the overall value of this Disaster Recovery Plan:

- The main body of this plan covers only the Scottsdale Center for the Arts Information Systems facility.
- The City Departments / Divisions information systems Disaster Recovery plan information is covered in the "Attachments" section of this document. A list of these City Departments / Divisions can be found in the SECTION 4 Index.
- Each City Department / Division is responsible for maintaining their own Disaster Recovery information. The Information Systems Department will add the City Department / Division DR plans as attachments to this document.
- The City of Scottsdale IS organization will research possible hot site, cold site, and / or workable reciprocal agreements with other organizations to create a more stable disaster recovery plan. These options are reviewed in Appendix K.
- The City of Scottsdale's IS organization will update and distribute this document to the Emergency Management Team, the Team Captains, and the City Department / Division representatives every six months.
- The Technical documentation referred to in this document will be kept up-to-date and stored off-site at the Data Pros Company.
- The Disaster Recovery Checklists (Appendices F and O) will be reviewed by the appropriate assigned team captains and updated before the next printing of this document.



digital city | search | services | human resource systems
www home | calendars | forms | teams | news | budget

Thank you for visiting our site.
Information Systems welcomes your [feedback](#)

For the City, business resumption planning is crucial. Disruptions in service delivery may not impact the fiscal health of the City, but the inability to provide services such as water, fire suppression, traffic control, or police response would negatively impact the health and safety of the citizens of Scottsdale. In addition, there are other functions such as the City's Municipal Court that provide critical services to citizens. Social services such as Senior Centers, after school programs, and the various assistance programs offered at Vista del Camino and the Paiute Neighborhood Center also serve a vital role in the community.

The City also needs to consider legal requirements such as records retention policies when considering whether or not a plan is necessary. Many of these records are not stored in a fashion to facilitate recovery should a building suffer smoke or water damage. In some cases, the data stored on desktop computers may be the only source of the record.

A good business resumption plan covers several basic areas. The following is a brief outline of what should be in a plan:

1. Identification of critical business functions through a business impact analysis.
2. Identification and documentation of critical business processes and tasks.
3. Identification and documentation of the resources needed to implement the plan.
4. Identification of teams responsible for carrying out the plan.
5. Procedures for periodic testing and maintaining the plan.

An effective plan affects the entire organization and requires sufficient funds to develop, maintain, and update as changes occur. Therefore, it is imperative that support and commitment come from the highest level of management within an organization. Professional literature ranks the lack of management support as the most serious threat to business resumption planning efforts.

We believe that many of the elements missing during our audit can be attributed to the fact that there is no citywide directive for adequate planning and no one individual assigned to ensure that the disparate efforts that do exist are coordinated. As such, the IS Department is limited in what it can accomplish as part of its Disaster Recovery Plan. Without full cooperation from all user departments, business risk assessment efforts cannot be accomplished.

City Needs to Ensure That Critical Business Operations Can Continue to Be Provided

There are several professional organizations that develop standards for business continuity planning. For example, DRI International has established a common body of knowledge and standards as well as a certification program. As well, ISACF includes continuity planning as one of the control objectives for information technology (IT). According to organizations such as these, the following factors should be in place to increase the success of any efforts undertaken toward business resumption planning:

- Support from both the governing body and top management with clear directives to the operating units setting out the requirement for a plan.
- Assigned staff and dedicated funds.
- Inclusion of all aspects of the organization, not just those reliant on computers.
- Identification of all vital records and development of a comprehensive backup policy.
- Documented recovery strategies based on the impact of the loss to the organization and required periodic testing with results reported to management.
- Maintenance of a recovery manual to ensure that it is reasonably current and available under any circumstance.

We used professional standards and guidance from these organizations to complete this audit. Our work led us to conclude that the City does not have a sufficient framework in place to quickly respond and recover from a disaster that would impact critical business functions. We found that the City does not have:

- A policy statement addressing the organizational commitment to ensuring continued business operations.
- An assigned individual who is responsible for ensuring that the City has an appropriate business resumption plan, an adequate awareness program, and sufficient training to implement the plan.
- Assigned staff and dedicated funds sufficient to maintain a plan, conduct the necessary awareness and training programs, and provide the means of developing periodic updates to any documented plan.

- A process that requires identification of vital records and assurance that those records can be recovered or restored.
- A requirement that directs each business unit to develop a plan.
- A written, tested citywide business resumption plan that would ensure minimum impact on services in the event of a major interruption.

Without standardized business resumption planning, critical services may not be recovered and restored to operating condition within a timely manner. As well, the City is less likely to have the appropriate documentation to protect against legal recourse or support the decisions made by staff.

We recommend that the City Manager develop a business resumption planning program that, at a minimum, includes:

1. A policy statement that clearly expresses the organization's commitment to ensuring continued business operations. This policy statement should be approved by Council and incorporated into the City Code.
2. A requirement for development of a business resumption plan that defines the roles, responsibilities, and approval process for the plan. This plan should be based on a risk assessment and impact analysis. At a minimum the plan should include:
 - Guidelines on how to use the plan.
 - Emergency procedures to ensure safety of all staff members.
 - Response procedures meant to bring systems back to the condition before the incident or disaster.
 - Recovery procedures to bring the systems back to the condition before the incident or disaster.
 - Procedures to secure and reconstruct the site.
 - Coordination procedures with public authorities.
 - Communications procedures.
 - Critical information on continuity teams, affected staff, customers, suppliers, public authorities, and media.
3. Assignment of one individual within the organization with the responsibility of ensuring the development and maintenance of the plan as well as the authority to implement the plan, if necessary. This individual should be required to be a certified business continuity professional.
4. A requirement that each business unit establish responsibility for plan development, activation, and maintenance.

5. A requirement for the City's Risk Management Director to participate in the development of the citywide plan.

Information Systems Disaster Recovery Plan Could Be Enhanced

Prior to 1999, the City did not have a disaster recovery plan that addressed the existing City's computer operations and network. The lack of such a plan was noted in the external auditor's management letter delivered as part of the audited financial statements for FY 1997/98. Concerns related to the Year 2000 threat also increased the awareness of the need for adequate disaster recovery planning to ensure that critical functions impacted by computer operations could continue.

To respond to these concerns, the IS Department elevated the issue of disaster recovery planning. A consultant was brought in to help draft a plan, and the IS General Manager/CIO assigned the responsibility for the plan to a manager within the department. This plan has been updated approximately every six months since its development.

To complete our review, we looked at the assignment of responsibility for the plan, the efforts to update it, and the process in place to implement it in the event of a disaster or other unforeseen event. We found that the efforts undertaken by the department are a good start in providing the foundation for a continuity plan. We did note, however, that the efforts could be enhanced with the inclusion of additional policies and procedures.

The Information Systems Department has Created the Foundation for a Business Resumption Plan

When the IS Department created a disaster recovery plan, input was solicited from other City departments/divisions. As well, departments/divisions were encouraged to add information specific to their area. To date, several departments have added portions to the IS Plan.

This Plan identifies all operating systems and third-party services such as equipment maintenance vendors used by the IS department. All data files supported by the network are identified, as are all types of equipment and special supplies. IS has documented minor instances that occur within their operation within the Plan.

As well, periodic updates have been undertaken as suggested by professional organizations. As changes are made the information is updated and stored in a disaster recovery folder on the IS server. Approximately every six months,

this information is used to update the City's Intranet as well as the manual that is printed and distributed. This information is backed up daily and stored in-house as well as offsite.

We noted that, while not a formal job assignment, the IS General Manager/CIO included responsibilities for disaster recovery planning within the performance plan of the manager assigned these duties.

Additional Policies and Procedures Would Enhance the Efforts

One of the more important standards in continuity planning relates to the maintenance of the plan. A plan that is allowed to get stale or no longer reflects current organizational priorities can create more issues than not having a plan at all.

We noted that the Plan currently used by IS was not developed in conjunction with a citywide risk assessment and business impact analysis to identify critical business processes or technology applications. Instead, the Plan is based on recovery priorities identified in 1999 as part of the Year 2000 efforts. Moreover, we noted that departmental plans, attached to the IS Plan, do not address the timeframe for recovery. As well, there is no standardization within the plans submitted by departments, and these plans do not consider other business processes that are needed to support the departmental plan.

We found that there are no scheduled tests of the plans to ensure that the manual processes or alternative steps can be achieved. The only testing to date involved preparations in 1999 for the Year 2000 threat. Additionally, we found that there is no process that would ensure follow-up on issues identified during testing. For example, during the testing in 1999, the disaster recovery coordinator discovered that the steps outlined for contact of staff were not sufficient. He found that while there was an emergency call list, there was no guarantee that someone would be available to answer the phone. As a result, pager numbers were added to the list. However, we found that there is no documentation to indicate that the numbers are kept current.

Also, while the IS Department takes steps to document minor instances, the recovery process used to respond to those instances is not documented. There is no indication of an after-the-fact evaluation to consider potential changes to the Plan. We found that the Plan includes a flowchart indicating that the final step should be to analyze the effectiveness of recovery and update the Plan as necessary. But, this process is not identified in the procedures.

We found that procedures within the IS Department would not ensure that every employee who is expected to respond to an incident is properly trained. There is no indication of ongoing training and no formal instructions provided to new employees. We noted one situation in which a new employee was added to the updated Disaster Team calling list. This employee had not received any instructions regarding the Plan nor had he received any documentation regarding the Plan.

Finally, we noted that the IS Disaster Recovery Plan does not provide for an alternative processing site or provide sufficient assurance that alternative equipment can be obtained and brought online within a required timeframe to be able to restore critical functions. As currently outlined, the planning for alternative sites is limited to discussion regarding the use of a cold site. According to the Plan, the site would have to be identified by Facilities Maintenance at the time of a disaster. There is no indication that Facilities Maintenance management is aware that this is their responsibility.

Even if an alternative cold site could be identified, there are many obstacles to getting an alternate site functional in a short timeframe. Appropriate hardware such as data lines and adequate power sources must be available or quickly brought to the site. The environment within the facility must be appropriate to handle the additional equipment to avoid degradation of service levels. Other items such as voice communications, operating systems, and specialized equipment must also be considered. We found that IS has not effectively planned for the acquisition and installment of the equipment and ancillary hardware. For example, computer equipment is purchased using state contracts or other contractual arrangements that do not provide for fast replacement when necessary.

According to the individual serving as the disaster recovery coordinator, he has recommended establishing an alternate site. He suggested using a Capital Improvement Project for funding but the proposal did not receive a high enough priority ranking. As well, we were advised that IS plans to review maintenance contracts to see if an agreement for recovery or replacement of equipment can be expedited.

We recommend that the City Manager require the IS General Manager/CIO to develop a citywide information systems disaster recovery program that would, at a minimum, include:

1. Identification of a specific individual assigned as the Disaster Recovery Officer and development of a job description that would include disaster recovery responsibilities. This individual should be required to implement policies and procedures that incorporate all appropriate

elements outlined by ISACF. As well, the individual should be required to be a certified business continuity professional.

2. Completion of an enterprise-wide risk assessment of all applications using the City's network or supported by IS to determine minimum acceptable time for recovery of the City's network and/or server farm.
3. Development of a best case scenario regarding the time to provide service should the SCA building become inaccessible or sustain sufficient damage to impact portions of the network.
4. Identification of an alternative computer operations center and development of strategic plans for bringing that site online, if necessary.
5. Renegotiation of current contracts to ensure replacement of critical equipment within an established timeframe.
6. Development of boilerplate language for inclusion in future contracts for critical technology-related components to ensure availability of replacement equipment.
7. A formal meeting, after each incident or successful resumption, to review recovery procedures and modify the plan, if necessary.
8. Development and implementation of an annual refresher/awareness program to ensure that employees are aware of specific requirements.

OBJECTIVES, SCOPE, AND METHODOLOGY

The objectives of this audit were to determine if:

- The City has appropriate senior level support for the development of a business resumption plan.
 - City Council should adopt a policy statement that clearly expresses the organization's commitment to ensuring continued business operations.
 - The City Manager should require that each business unit establish responsibility for plan development, activation, and maintenance at the business unit level.
- The City has an operational, tested plan that would ensure minimum impact on services in the event of a major interruption.
 - City management should develop a plan that defines the roles, responsibilities, and the approval process.
 - The plan should be based on a risk assessment of the business processes and a business impact analysis.
- The City has the appropriate framework in place to implement the plan.
 - The plan should include:
 - Guidelines on how to use the plan.
 - Emergency procedures to ensure safety of all staff members.
 - Response procedures meant to bring systems back to the condition before the incident or disaster.
 - Recovery procedures to bring the systems back to the condition before the incident or disaster.
 - Procedures to secure and reconstruct the site.
 - Coordination procedures with public authorities.
 - Communications procedures.
 - Critical information on continuity teams, affected staff, customers, suppliers, public authorities, and media.
 - City management should implement change control procedures to ensure that the plan is up-to-date and reflects actual business requirements. Maintenance of the plan should be aligned with organizational change and human resource procedures.
 - City management should periodically test the plan to ensure its adequacy. Testing should encompass documentation, reporting test results, and action plans to implement identified concerns.
 - City management should ensure that all concerned parties receive regular training sessions regarding the procedures to be followed in case of an incident or disaster.

- The Information Systems Department has an operational, tested plan that would ensure minimum business impact in the event of a major interruption.
 - IS should develop, in cooperation with business process owners, a plan that defines the roles, responsibilities, and the approval process.
 - The plan should be based on a risk assessment of the systems and a business impact analysis.
- The Information Systems Department has the appropriate framework in place to implement the plan.
 - IS should develop a written plan that includes:
 - Guidelines on how to use the plan.
 - Emergency procedures to ensure safety of all staff members.
 - Response procedures meant to bring systems back to the condition before the incident or disaster.
 - Recovery procedures to bring the systems back to the condition before the incident or disaster.
 - Procedures to secure and reconstruct the site.
 - Coordination procedures with public authorities.
 - Communications procedures.
 - Critical information on continuity teams, affected staff, customers, suppliers, public authorities, and media.
 - IS should provide for change control procedures to ensure that the plan is up-to-date and reflects actual business requirements. Maintenance of the plan should be aligned with change and human resource procedures.
 - IS should periodically test the plan to ensure its adequacy. Testing should encompass documentation, reporting test results, and action plans to implement identified concerns.
 - IS should ensure that all concerned parties receive regular training regarding the procedures to be followed in case of an incident or disaster.
 - The plan should identify the critical application programs, third-party services, operating systems, personnel, supplies, data files, and timeframes needed for recovery after a disaster occurs.
 - IS should ensure that the methodology incorporates an identification of alternatives regarding the backup site and hardware as well as a final alternative selection. If applicable, a formal contract for these types of services should be concluded.

- IS should ensure that, on successful resumption of the information services function after a disaster, the adequacy of the plan is assessed, and the plan is updated accordingly.

To complete this evaluation, we used control objectives for information and related technology outlined by ISACF. The Foundation considers these objectives "best practices" for ensuring continuous service while minimizing business impact. We also used standards promulgated by DRI International.

We interviewed staff, reviewed the City's Administrative Guidelines, City Charter and Code, job descriptions, and Emergency Operation Plan to gain an understanding of the City's business resumption policies. In addition, we analyzed the Disaster Recovery Plan maintained by the IS Department. Audit work was conducted in accordance with generally accepted government auditing standards as they relate to expanded scope auditing in a local government environment and as required by Article III, Scottsdale Revised Code §2-117 *et. seq.* Fieldwork took place from June to July 2001. Discussion of the methodology to evaluate each objective is on the following pages.

Objective 1: Determine whether City has appropriate senior level support for the development of a citywide continuity plan.

Criteria: The City Council should adopt a policy statement that clearly expresses the organization's commitment to ensuring continued business operations.

Method: This work will be accomplished by searching the Intranet for positions containing disaster recovery or performance evaluations. Additionally, request IS Support Manager performance plan. Review the Scottsdale Revised Code for any references to business continuity or disaster recovery requirements.

Results: The IS staff member assigned as the disaster recovery coordinator fills a position titled "IS Support Manager." On July 3, 2001, obtained performance plan for this individual. It included two tasks pertaining to disaster recovery projects.

- IS Contingency Plan – (six month updates-- next update February 2001).
- Citywide Risk Impact Analysis – (December 2000).

Located the job description on the Human Resource Systems (HRS) Intranet site. This job description has not been updated since October 1996 and contains no reference to the duties of disaster recovery. Also discovered that there was no such active job title or salary range on the HRS Intranet site for this particular job classification. According to the IS Support Manager, HRS is in the process of rewriting the job description, and it will include the duties associated with disaster recovery.

Contacted the Emergency Services Officer regarding the City Emergency Plan. The Emergency Service Officer sent a copy and indicated that they would be updating it this fall for several reasons. According to the Emergency Service Officer, the Plan is to be updated every three years. He also identified the reorganization within the City as another reason to update the Plan. He also stated that he does not keep detailed department plans nor is he responsible to ensure that they are effective. Reviewed the emergency response plan submitted by the Emergency Service Officer and found that it does not address resumption of City operations.

Also reviewed the job description for this position and found, similar to the IS Support Manager, that the description has not been updated since October 1996. It does not include any responsibilities associated with recovery of City operations.

Also contacted the Risk Management Director and reviewed the job descriptions associated with Risk Management. None of these address business continuity or recovery.

Objective 2: Determine if the City has an operational, tested continuity plan that would ensure minimum impact on services in the event of a major interruption.

Criteria: City management should develop a business continuity plan that defines the roles, responsibilities, and the approval process.

Method: Search the Intranet and City policies and procedures to determine if such a plan exists.

Results: No plan exists to test.

Objective 3: Determine if the City has the appropriate framework in place to implement the continuity plan.

Criteria: City management should develop a business continuity plan that includes necessary steps to continue to operate during a disaster and recover quickly.

Method: Search the Intranet and City policies and procedures to determine if such a plan exists.

Results: No plan exists to test.

Objective 4: Determine if the Information Systems Department has an operational, tested plan that would ensure minimum business impact in the event of a major interruption.

Criteria: In order for a disaster recovery plan to be effective, a risk assessment and business resumption plan must be performed.

Method: This work will be accomplished by searching the plan or policies and procedures. Meet with IS staff assigned responsibility for disaster recovery to determine if the plan would ensure minimum business impact in the event of a major interruption.

Results: On July 11, 2001, reviewed the recovery plans for applications supported by IS and found there is no established priority for recovery. Additionally, there is no backup site currently planned or available in the Plan.

There is a business impact analysis being conducted. However, support from other City departments is less than adequate. Moreover, several departments have not even responded to the consultant's questionnaires.

Objective 5: **Determine whether IS has an appropriate framework in place to implement the division's continuity plan.**

Test 1: **Review plan for framework.**

Criteria: In order for a disaster recovery plan to be effective, all processes and services must be identified.

Method: This work will be accomplished by searching the plan or policies and procedures. Meet with IS staff to determine if the Plan includes guidelines on how to use the Plan.

- Guidelines on how to use the plan.
- Emergency procedures to ensure safety of all staff members.
- Response procedures meant to bring systems back to the condition before the incident or disaster.
- Recovery procedures to bring the systems back to the condition before the incident or disaster.
- Procedures to secure and reconstruct the site.
- Coordination procedures with public authorities.
- Communications procedures.
- Critical information on continuity teams, affected staff, customers, suppliers, public authorities, and media.

Results: On July 11, 2001, reviewed the individual pieces of the plan. They were all addressed. The plan includes:

- Guidelines on how to use the plan.
- Emergency procedures to ensure safety of all staff members.
- Response procedures meant to bring systems back to the condition before the incident or disaster.
- Recovery procedures to bring the systems back to the condition before the incident or disaster.
- Procedures to secure and reconstruct the site. However, this was limited to directions to contact Facilities Maintenance.
- Coordination procedures with public authorities. This was addressed in the emergency call list.
- Communications procedures were also addressed in the management checklist.
- Critical information on continuity teams, affected staff, customers, suppliers, public authorities, and media. This was available.

Test 2: **Review change control procedures to ensure that the plan remains up-to-date.**

Criteria: In order for a plan to be effective, the entire plan needs to be current.

Method: This work will be accomplished by reviewing the process for keeping the plan up-to-date.

Results: On July 11, 2001, reviewed the section covering maintenance of the plan. The area showed the original issue and four updates approximately six to seven months apart.

Also discussed the process for updates with the IS Support Manager. The computer operators, responsible for updating the City phone list, update the Disaster Team phone list at the same time. Noted that the phone list is not current and does not reflect recent changes within the IS Department.

Plan changes are made online and stored in the Disaster Recovery Directory of the IS share server. These changes are also printed and inserted in the Plan maintained in the IS

Support Manager office as well as the Plan kept offsite. The new page is tagged for update when the full update is done approximately every six months.

Test 3: Review historical records of testing to determine sufficiency.

Criteria: In order for a plan to be effective it needs to be tested on an established timeframe.

Method: This work will be accomplished by searching the plan or policies and procedures. Meet with IS staff to determine if periodic tests have been conducted.

Results: On July 11, 2001, reviewed the test and education section of the plan. Noted that the plan included a section that identified all incidents since November 11, 1998. This list included the date, the person that handled the incidents, and comments as to what happened.

Asked the IS Support Manager if a process existed to review the plan after an instance to determine if the plan adequately addressed the issue or if it should be modified. He indicated that there is no formal procedure to do this. However, he stated that IS staff usually meets to discuss what happened and determine if they could have done a better job solving the problem. If there is a better way to correct the problem, the plan is updated.

He also stated that the only actual test was in 1999. At that time they discovered that very few people answered the phone identified in the call list. To correct this problem, pagers were added to the list.

Test 4: Review historical training and future schedule of training to ensure that all concerned parties receive periodic training regarding procedures.

Criteria: In order for a plan to be effective, all concerned parties need to receive regular training on its use.

Method: This work will be accomplished by searching the plan or policies and procedures. Meet with IS staff to determine if training on the use of the plan has been conducted.

Results: On July 11, 2001, reviewed Plan for training procedures. The Plan did not address periodic training.

Discussed training with the IS Support Manager. He indicated that the City's outside consultant conducted some training in 1999. He stated that no training was undertaken in the last year as the Plan has not changed significantly. He also stated that all new hires that potentially will be impacted by the Plan receive a copy.

Contacted two new IS employees and inquired about the Plan. One stated that a copy of the plan was received but there was no training on how to implement it. The second employee stated that no copy was received and no training had been provided.

Test 5: **Review the Plan to ensure that IS has identified all critical application programs, third-party services, operating systems, personnel, supplies, data files, and timeframes needed for recovery.**

Criteria: In order for a plan to be effective, all processes and services must be identified and stored offsite.

Method: This work will be accomplished by searching the plan or policies and procedures. Meet with IS staff to determine if the plan identifies critical application programs, third-party services, operating systems, personnel, and supplies, and data files.

Results: On July 11, 2001, reviewed the applications supported by IS and found that the plan does not establish priority for recovery. The plan relies on the Y2K project risk rating but this list was not currently available. There is an application database that lists most, but not necessarily all, IT technology applications in the City. Currently, this database does not address priority or recovery time.

The plan does address third-party and personnel, it also addresses data files and supplies. Operating systems are also addressed in the data files backup procedures. These systems are backed up weekly and stored both on-site and offsite in a locked box for easy retrieval.

Testing of the actual offsite backup procedures was conducted July 13, 2001. To complete this testing, Clearpath and enterprise-wide server back-up tapes were identified for verification. When the tapes were returned from the offsite vault, one set was missing. The vendor was called and required to bring the tapes in question back that day. The other two sets, one for the Clearpath and one for the Enterprise, were sufficient to determine that the offsite storage did exist and was working.

Test 6: Review the Plan for backup site and hardware.

Criteria: In order for a disaster recovery plan for IS to be effective, a backup site must be identified and planned for. Additionally, replacement equipment must be scheduled.

Method: This work will be accomplished by searching the plan or policies and procedures. Meet with IS Support Manager to determine if the Plan identifies timeframes needed for recovery, backup site, and replacement hardware.

Results: Reviewed the Plan and determined that the issue of an alternative computer operations center is addressed with instructions to contact Facilities Maintenance for space should an alternate site be necessary.

According to the IS Support Manager, he does not have the necessary data on which to make a determination on how critical an alternative site is. To date, no user department has established a set timeframe and priority that would drive the determination as to what type of alternative site should be available. As well, he is uncertain as to the City's expectation for citywide recovery and resumption.

Also reviewed contracts currently used for hardware purchases and found that the state contracts do not address replacement hardware.

Test 7: Review recovery procedures for adequacy.

Criteria: In order for a disaster recovery plan for IS to be effective, recovery procedures need to be documented and evaluated for possible updating of the plan.

Method: This work will be accomplished by searching the plan or policies and procedures. Meet with IS Support Manager to discuss procedures to update the Plan after successful resumption.

Results: On July 12, 2001, reviewed the plan and found that it includes a flow chart indicating that the final step is to analyze the effectiveness of recovery and update the Plan if necessary. Noted, however, that this process is not discussed in the body of the Plan and there are no procedures outlined that would result in this review.

Discussed follow-up procedures with the IS Support Manager to determine if the Plan has been evaluated after instances. He indicated that there is no formal procedure to do this but, historically, IS personnel met to discuss problems and remedies. If the evaluation resulted in identification of a better way to handle the situation or correct the problem, the Plan was updated.


He provided an example of the action taken during the testing undertaken in 1999. In this situation, IS discovered that very few people answered their desktop phone. As such, during the evaluation phase, a determination was made to add pagers to the phone list.

APPENDIX A

Management Response

December 4, 2001

To: Cheryl Barcala, City Auditor

From:  David L. Ellison, Assistant City Manager

Through: Jan Dolan, City Manager 

Re: Management Response to Business Resumption Report No. 0162

Transmitted herewith is the management response to Business Resumption Report No. 0162. The audit process that resulted in this report was initiated during the summer of 2001. The report was presented to the Office of the City Manager on or about September 25, 2001. The focus is an evaluation of the city organization's capacity and ability to respond to and recover from a disaster or unforeseen event that could disrupt critical business functions and other city services and programs. Report No. 0162 is written from an internal audit perspective, and city management is sincerely appreciative of the specific and broader insights, findings and recommendations offered in this and other evaluations of our business processes, procedures and practices.

General Response & Update:

The overall view of the city manager and leadership team members most directly accountable for a response is that the report raises important questions and provides useful insights at a time when citizens, all service recipients and policy-makers expect and deserve increased emphasis on always critical emergency preparedness activities and efforts. Consistent with this ever-present and growing expectation is a city manager and leadership team philosophy that public safety be treated as the most essential of many important city services.

A specific example of the commitment to public safety is city manager authorization of the expeditious filling of police department vacancies at a time when other city recruitments and positions are being delayed, re-allocated to areas of higher priority or potentially eliminated altogether. While allocation of ample resources for police and fire services continues to be a top organizational priority, senior management is also taking steps to ensure that said resources are being used wisely and in a manner most closely aligned with new demands and City Council goals.

Page 2
Management Response

The next important piece of information to convey is the fact that the city manager has directed key senior managers in the organization to make development and implementation of a comprehensive emergency management program an ongoing, priority responsibility. The program will be revised to fit changing needs. A related directive is to significantly enhance the quality and amount of information provided to the public in regards to proper steps to follow and sources to contact in the event of an emergency. Key management personnel being held directly accountable for this effort include Doug Bartosh, chief of police, Dee Taylor, executive assistant chief of police, David Ellison, assistant city manager, Marc Eisen, emergency services director and Pat Dodds, communications and public affairs officer.

The Chief of Police has demonstrated his commitment to creation of a viable, comprehensive and sustainable emergency preparedness plan and structure by significantly reshaping the role of Assistant Chief Taylor. She is the second highest ranked member of the department. Her role now includes lead responsibility for the entire organization's emergency management work program. The emergency services director and recently hired workplace security coordinator now report directly to Assistant Chief Taylor. These two individuals are also key members of a citywide emergency planning and implementation team called the ***Emergency Safety and Preparedness Committee (ESAP)***. Assistant Chief Taylor leads this recently established team. Research, training and emergency planning activities have intensified the past few weeks, and the group has determined that the core elements of the organization's comprehensive emergency management program are to be as follows:

- Emergency Preparedness (Planning, Preparation, Training)
- Emergency Response (Successful Activation When Event Occurs)
- Business Resumption (Restoring Priority Systems & Services)

Each of the above elements requires significant action plans that may overlap. The recommendations contained in Audit Report NO. 0162 are being taken into consideration, and Y2K planning efforts may also prove useful to a certain extent.

Page 3
Management Response

Response to Specific Issues & Recommendations:

Issue/Recommendation # 1

The City needs to develop a business resumption plan to ensure that there is a coordinated response to an unforeseen event that would disrupt critical business functions.

Management agrees that there is a need for development and regular update of a comprehensive emergency management program, which includes how to continue and resume business during and after an unforeseen event. Important policy, management and resource allocation decisions must be identified and made to accomplish this. Dee Taylor, executive assistant chief of police is now responsible for this critical activity on an ongoing basis. Other key executives are accountable for the success of these immediate and ongoing efforts, and a citywide Emergency Safety & Preparedness Committee (ESAP) has been established under Assistant Chief Taylor's leadership and coordination. The ESAP Committee is comprised of representatives from every key department and function needed during an emergency. The team was formed in early November and has been meeting every two weeks. The ESAP committee is using Audit Report No. 0162 and Y2K results and recommendations as platforms for future work. Planning, research and training information is also being gathered from local, regional, state and national public and private sector resources.

A detailed action plan is being finalized for presentation to the city manager. It will identify estimated implementation costs and alternatives to recommendations in Audit Report No. 0162, among other things.

Issue/Recommendation #2

The City's Emergency Response Plan has not been updated since 1998. The plan is considered supplemental to the City code and has the effect of law during a situation in which an emergency is declared. It is therefore imperative to keep the plan current, particularly when there are organizational changes.

The Emergency Services Director reports that the current plan became effective July 6 1999, upon review and approval of the Mayor and City Council. Past practice has been to update the plan every three to four years unless changes in the city organization or federal or state requirements create need for more immediate revisions.

Page 4
Management Response

A more comprehensive plan is being developed for review and approval as part of the work being done by Assistant Chief Taylor and the ESAP team. This preparedness plan is a key component of the overall emergency management program referred to on page two. It will be reviewed every year for completeness and applicability, and updated as appropriate.

Issue/Recommendation #3

Citywide awareness and training programs are not provided annually and the Emergency Services Director assumes no responsibility for ensuring that departmental plans are current, sufficient and supplemental to the citywide plan. Expand the duties of the Emergency Services Director to ensure implementation of annual, effective training and coordination of departmental plans to supplement the citywide plan.

Management agrees that there is a need for relevant, effective and more frequent training. This training shall be mandated for key personnel and operations identified in the Emergency Safety and Preparedness Action Plan. Assistant Chief Dee Taylor is the top leader responsible for a comprehensive emergency management program, with strong support from a number of executives and the emergency services director.

Issue/Recommendation #4

The City is not maintaining current job descriptions. Job descriptions for IS Support Manager, the Emergency Services Officer, Risk Management Director, and Risk Management Manager have not been updated since 1996. The position of IS Support Manager is no longer reflected on the City list of active titles and pay range.

Recommend that the City Council instruct the City Manager to direct the Human Resource Systems General Manager to initiate a process to update all job descriptions and ensure that job titles/duties assigned to City employees are correctly reflected in both job descriptions and classifications.

The Human Resources Department is reviewing this matter and will make it a priority to update job descriptions and classifications that are critical to successful implementation of a comprehensive emergency management program. Management feels confident that key personnel are prepared to contribute as required. An effective emergency management program and proper training are the keys to making sure everyone understands and executes roles during and after an event.

Page 5
Management Response

Issue/Recommendation #5

The City has the start of a business resumption plan in the Disaster Recovery Plan maintained by the City's Information Systems Department (IS). This plan would help facilitate the recovery of the City's computer network, if necessary. However, the plan, as it currently exists, is not sufficient to ensure timely restoration of computer operations and would not ensure a coordinated response to the disaster or other event.

Management understands the distinction between a disaster recovery plan and a more comprehensive business resumption plan. The audit report has provided valuable information about complex and basic issues related to emergency preparedness, business resumption and daily operation of business systems located across the organization. IS disaster recovery efforts are being incorporated into citywide emergency management program activities. A soon to be conducted strategic planning process for Information Systems operations should also prove helpful in this regard.

Issue/Recommendation # 6

The individual within the IS Department responsible for the Disaster Recovery Plan, is not charged with responsibility for, or given authority to develop a citywide business resumption plan. One individual, that is a disaster recovery professional, should be given responsibility and authority.

Executive Assistant Chief Dee Taylor has been delegated lead responsibility for citywide emergency management program efforts. Business resumption is a core component of a three-pronged strategy (planning, response, recovery). IS disaster recovery planning efforts are being incorporated into citywide efforts under operational direction of Rich Peterson, technology operations manager. Mr. Peterson is a senior manager, experienced and responsible for updating the IS plan every six months. He also coordinates training for the department's disaster recovery team and is a member of the Emergency Safety and Preparedness Committee.

Issue/Recommendation # 7

The City does not have a backup site for computer operations and it is estimated that it would take a minimum of thirty (30) days to restore portions of the network infrastructure.

IS management is in full support of an alternate site, be it "hot, warm or cold." Initial efforts are to identify a "cold site" location. Potential private and/or regional solutions will be evaluated by the IS team and ESAP Committee.

Page 6
Management Response

Issue/Recommendation # 8

Renegotiation of current contracts to ensure replacement of critical equipment within an established timeframe.

IS management will partner with the legal and purchasing teams in researching options available through current equipment and third party vendors. Replacement language may be included in any contracts being negotiated in the future if feasible.

Issue/Recommendation # 9

Development of boilerplate language for inclusion in future contracts for critical technology-related components to ensure availability of replacement equipment.

IS management advises that the City already has a high expectation for timely replacement of hardware though use of existing maintenance contracts. The department will explore this recommendation in cooperation with the legal and purchasing teams, and anticipates the need for a thorough cost/benefit analysis. The IS department further advises that catastrophic events on a nationwide scale are likely to quickly deplete hardware inventories and the capacity of vendors and knowledge workers, regardless of contract language.

Issue/Recommendation # 10

Completion of an enterprise-wide risk assessment of all applications using the City's network or supported by IS to determine minimum acceptable time for recovery of the City's network and/or server farm.

The IS Department's disaster recovery officer is responsible for facilitation of a process which will determine organizational priorities for bringing critical systems back online within a preferred timeframe.

Issue/Recommendation # 11

Development of a best case scenario regarding the time to provide service should the Scottsdale Center for the Arts building become inaccessible or sustain sufficient damage to impact portions of the computer network.

The IS Department disaster recovery consultant will assist with evaluating ways to reduce potential downtime. The IS effort should be completed within 120 days, and a timeline for looking at citywide services is being developed by the ESAP team.

Page 7
Management Response

Issue/Recommendation # 12

A requirement that each business unit establish responsibility for plan development, activation, and maintenance.

The new emergency management plan will include individual departmental plans.

Issue/Recommendation # 13

A formal meeting, after each incident or successful resumption, to review recovery procedures and modify the plan if necessary.

All involved city operations shall be included in debriefings held after each incident.

Issue/Recommendation # 14

Development and implementation of an annual refresher/awareness program to ensure that employees are aware of specific requirements.

Management agrees that this should be a component of the citywide emergency management program. Additionally, staff has found that "mock drills", based on different scenarios, provide the best opportunity for team members to practice implementing the elements of the disaster recovery plan. These exercises will be continued, at least annually and the Emergency Safety and Preparedness Committee will determine how to improve citywide Emergency Preparedness Training.

Issue/Recommendation #15

A requirement for the City's Risk Management Director participation in the development of the citywide Plan.

The Risk Management Director is actively involved in all current emergency management program related activities. He is a member of the Emergency Safety and Preparedness Committee and has provided the assistant city manager with considerable advice and research material upon request.

Page 8
Management Response

Issue/Recommendation #16

A policy statement that clearly expresses the organization's commitment to ensuring continued business operations. This policy statement should be approved by Council and incorporated into the City Code.

City management is committed to developing, implementing and maintaining a comprehensive emergency management program, which includes planning for continuation of business operations.

CC: Jan Dolan, city manager
Douglas Bartosh, chief of police
Dee Taylor, executive assistant chief of police
Mark Eisen, emergency services director
Carder Hunt, chief information officer
Barbara Burns, assistant city manager
Roger Klingler, assistant city manager
Ed Gawf, deputy city manager
Pat Dodds, communications and public affairs officer